(emphasis added). Instead, the system of Vicard requires that a chip-key be supplied to a lock circuitry from a source external to the chip (Vicard, col. 4, lines 43-45).

In response, the Examiner asserted that "the key stored in hashed format is the release key since it is used to determine whether the circuit is to be unlocked or not. The hash, encrypted key is stored within the chip and a received encrypted key is submitted to the same hash function to later determine if a match exists (Vicard, summary of the invention, columns 3-6). Applicant's arguments are not persuasive. Vicard clearly teaches having stored a hash of a key (a key on its own right)".

Applicant then noted that even if Vicard did disclose storing a key, Vicard does not disclose storing *both* a key and a lock as recited in claim 1. Vicard only discloses storing a signature of a correct chip-key in the register 25 shown in Fig. 1 (see Vicard, col. 4, lines 62-66).

Vicard discloses inputting an external chip-key and decrypting the externally input chip-key at the secure communications module 20, such that a first intermediate chip-key output IV1 is sent to the one-way hash function module 26 to be hashed. The intermediate hashed chip-key IV2 is then compared to the stored signature of a correct chip-key at the comparator 27. While the Examiner asserts that the stored signature of Vicard discloses the security release key recited in claim 1, applicant respectfully submits that even if the stored signature were equivalent to the stored release key of claim 1, which it is not, Vicard would then fail to disclose or suggest storing the security registration lock in a nonvolatile storage, as recited in claim 1. Vicard only discloses storing one element, the signature. Consequently, regardless of which element (a key or a lock) is stored in Vicard, the other element is not stored.

In response to applicant's Response filed on January 24, 2007, and summarized above, the Examiner asserts in the Advisory Action mailed February 12, 2007, that applicant's arguments are unpersuasive because "Vicard teaches storing a signature of a correct chip-key and a decryption key, since the input is received in an encrypted form (col. 3, lines 40-50), decrypting the input to

produce a first value, and applying a hash function to this value to produce a second value (col. 4, lines 43-61, and claims 1-6), Vicard further teaches using 2 or more chip-keys (col. 6, lines 20-36)."

Applicant initially submits that by asserting that the hash encrypted key that is stored in the chip is the release key, and that a received encrypted key is submitted to the same hash function to later determine if a match exists, the Examiner takes the position that "a key" (the hash, encrypted key, as a release key) is compared with another "key" (received encrypted key). This interpretation is not consistent with the concept of a security "lock" and "key" configuration as disclosed and claimed by applicant, where a received "key" is compared with a stored "lock." In such configurations, when a received key matches a stored lock a security function is released. Instead, the Examiner appears to assert that a received "key" is compared with a stored "key," which is not what applicant claims

Additionally, applicant respectfully submits that the Examiner has failed to address applicant's arguments that Vicard requires that the chip-key be supplied to the lock circuitry from externally of the chip (see, e. g. , column 4, lines 43-45 of Vicard), i.e., *not* stored *in the chip.*

The hash encrypted key that is stored in the chip (i.e., the "signature of the correct chip-key for the chip concerned") "*is stored in register 25 of the lock circuitry*" (emphasis added: see, applicant's Fig. 1, and Fig. 3 and col. 4, lines 65-66 of Vicard).

Furthermore, Vicard discloses that "[i]n order to ascertain whether an input chip-key is the correct one to unlock the particular chip 10 concerned, the lock circuitry further comprises a one-way function block 26 that subjects the chip-key output as IV1 from block 20 to the one-way function (in this case, the SHA) used to form the chip-key signature held in register 25. The resultant intermediate value hash encrypted key that is stored in the IV2 output by block 26 is then compared in comparison block 27 with the signature stored in register 25; if a match is found, the comparison block 27 outputs an enable signal on line 19 to cause operational enablement of the functional block 12." (Vicard, col. 5, lines 10-24). In other words, the signature of the chip-key

(i.e., the Examiner's indicated "hash, encrypted key [wh.ch] is stored within the chip") that is stored in register 25 of the lock circuitry represents a "lock," while the input chip-key represents a "key." Accordingly, if the input "key" matches the stored "lock," the user gains access to the functional block.

In relation to claim 1, the signature of the chip-key of Vicard may correspond to the "security registration lock" that is stored in the at least one nonvolatile storage means (see applicant's Non-volatile register 13 of Figure 1 and paragraphs [0053] to [0055]). The chip-key of Vicard cannot correspond to the security release key of this invention because, in Vicard, the chip-key is input by a user (from a source external to the chip) in contrast to the features of claim 1, where the security release key is stored in the at least one memory region, each one of said at least one memory region being provided in the at least one memory cell array block.

As noted in applicant's specification, the conventional technique as shown in Figure 3 (which is noted above as being similar to the invention as disclosed by Vicard) has at least the following problems:

> First, in order to release the function limitation, it is necessary to externally input a function limitation release key. Accordingly, the above-described system *requires an external key storage device* for storing the function limitation release key. However, since the function limitation release key is retained external to the device, *the key must pass through an interfacing section every time access is requested, independent of what sort of encryption technique may be employed in the communication path between the devices*, i.e., between the device shown in FIG. 3 and any other device within the system (e.g., the key storage device). *This may run the risk of the function limitation release key being intercepted during communication, or being directly read from the external key storage device.*
>
> Moreover, *complicated circuitry is required for encrypting signals exchanged between devices*, and particularly complicated encryption is required. Hence, complicated decoding circuitry within the device is required to provide protection against repetitive attacks; and
>
> Furthermore, in order to effectuate a good tamper prevention function, merely replacing a given semiconductor storage device with a semiconductor storage device having a tamper prevention function does not suffice. In addition, *the entire system*

must be redesigned to enable a good tamper prevention function" .

(Emphasis added). See, paragraphs [0009] to [0011] of applicant's specification; and col. 4, lines 43-61 of Vicard, wherein Vicard discloses the encryption and decryption that are required.

Furthermore, Examiner's assertion that the hash encrypted key that is stored within the chip is the claimed security release key is inconsistent with the teachings of Vicard and with the general concept of a "lock" and "key" arrangement as discussed above. To the contrary, it is pointed out that the hash encrypted key is stored in register 26 of the lock circuitry 11 of Vicard (Vicard, Fig. 1, and col. 4, line 65 to col. 5, line 9), such that Vicard does not disclose or suggest that the "key" (i. e., the security release key) is stored in the semiconductor storage device (i.e., in at least one memory region thereof).

Moreover, applicant's specification states that "... in the case of applications, such as BIOS or firmware, which function as ROMs during system operation and require no rewriting, a user of a system incorporating the non-volatile semiconductor storage devices according to the present invention *will not be conscious of the presence of the security function*" (emphasis added; applicant's paragraph [0067]). Vicard does not teach this feature, a chip-key must be input by the user such that the user is conscious of the presence of the security function.

In response to the Examiner's question regarding the role of the unauthorized user, applicant refers the Examiner to paragraphs [0060], [0069] to [0072], [0080] to [0082], and [0084] to [0093] of the specification.

Accordingly, since Vicard does not disclose or suggest all of the features of claim 1, claim 1 is allowable. Claims 2-10 depend from claim 1 and are allowable due at least to their dependencies.

Additionally, the Examiner asserts that "applicant's previous arguments failed to comply with 37 CFR 1.111(b) because they amounted to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references" (page 2 of the Action). Applicant respectfully submits that

applicant's arguments are directed at Vicard's failure to teach or suggest that both a "lock" and "key" are provided/stored in a semiconductor storage device as recited in claim 1. Instead, Vicard requires that the "key" be input by a user. Accordingly, applicant's arguments comply with 37 CFR 1.111(b).

Applicant respectfully requests that the Examiner reconsider the claims in light of the preceding remarks, and solicits an early action allowing the claims.

In the event the U.S. Patent and Trademark Office determines that an extension and/or other relief is required, applicant petitions for any required relief including extensions of time and authorizes the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to **Deposit Account No. 03-1952** referencing Docket No. **299002053200**.

Dated: February 26, 2007

Respectfully submitted,

By _____

Adam Keser
Registration No. 54,217
MORRISON & FOERSTER LLP
1650 Tysons Blvd, Suite 300
McLean, Virginia 22102
(703) 760-7301